-冬冬说无线-

无线802.1X认证排查及优化

H3C WLAN

802.1X协议是一种基于端口的网络接入控制协议（Port based networkaccess control protocol）。即在局域网接入设备的端口上对所接入的用户和设备进行认证，以便控制用户设备对网络资源的访问。

本次我们介绍在使用无线802.1x场景下，认证异常或超时的情况如何处理及排查，适用于采用EAP中继模式并结合认证服务器的远程802.1X认证。

802.1X认证排查及优化

1 确认故障范围

确认问题发生的范围，是全网大多数终端认证失败，还是只有个别终端异常。必要时，请尝试更换终端测试，比如PC、不同型号的手机。

2 确认故障类型

确认是否是802.1X认证失败？还是终端能认证成功，但是无法上网？可以通过AC上命令确定用户能否通过802.1x认证。部分终端在802.1x认证成功后，还必须获取ip地址，才能显示成功连接802.11网络。所以802.1X认证成功但是获取不到IP地址也可能导致误判为802.1x认证失败。

例如：通过命令查看1x认证用户信息，可以看到用户名、终端MAC地址、IP地址和在线时长。

```
[AC]display dot1x connection
Total connections: 1
User MAC address                : 6a6f-356a-89a7
AP name                     : wa6528
Radio ID                   : 1
SSID                    : 1x
BSSID                    : 3cd2-e5a2-d142
Username                     : 123
Anonymous username               : N/A
Authentication domain            : dm-1x
IPv4 address                  : 192.168.137.2
Authentication method            : EAP
Initial VLAN                  : 137
Authorization VLAN               : 137
Session timeout last from              : 2023/04/25 10:08:37
Session timeout period           : 86400 s
Online from                   : 2023/04/25 10:08:37
Online duration                : 0h 0m 5s
```

3 检查链路连通性

通过Ping操作判断认证设备与服务器之间是否可达，如果不通，说明到认证服务器的路由有问题，需要检查路由配置；检查防火墙是否放通1812和1813端口；检查认证服务器端口状态。

设备上通过查看Radius的状态也可以用来确认服务器连通性。

```
[AC]dis radius scheme rs-1x
RADIUS scheme name: rs-1x
 Index: 0
 Primary authentication server:
  IP  : 192.168.133.254              Port: 1812
  VPN  : Not configured
   State: Active (duration: 0 weeks, 4 days, 11 hours, 43 minutes, 58 seconds)
  Most recent state changes:
   2023/04/20 08:55:58 Changed to active state
  Test profile: Not configured
 Primary accounting server:
  IP  : 192.168.133.254              Port: 1813
  VPN  : Not configured
   State: Active (duration: 4 weeks, 5 days, 4 hours, 11 minutes, 51 seconds)
  Most recent state changes:
   2023/03/22 16:22:08 Changed to active state
```

4 根据设备上的日志看原因

查看在设备上产生的802.1X认证失败的原因：

```
Username=[STRING]-UserMAC=[STRING]-SSID=[STRING]-APName=[STRING]-RadioID=[STRING]-VLANID=[STRING]; A user failed 802.1X authentication. Reason: [STRING]. AAA processed authentication request and returned error code
```

AAA处理认证请求并返回错误码code，我们可以针对code取值判断可能是什么原因导致认证失败：

4：认证域不存在

8：认证域下的配置错误/服务器上配置的共享密钥与设备配置的共享密钥不一致/认证端口1812没有开启/服务器与设备网络不可达

26：用户名或密码错误/认证类型错误/服务器上没有添加设备IP地址/服务模板下认证域配置错误

5 检查AC上的关键配置

1） 检查无线服务模板下配置的WLAN用户接入认证模式是否为dot1x，检查认证域调用是否正确。

```
wlan service-template 1x
  ……
 client-security authentication-mode dot1x
 dot1x domain dm-1x
 service-template enable
```

2） 检查AC上802.1X系统的认证方法是否为EAP。

```
dot1x authentication-method eap
```

3） 检查AC上的认证域配置是否有误。

```
domain dm-1x
  authentication lan-access radius-scheme rs-1x
 authorization lan-access radius-scheme rs-1x
 accounting lan-access radius-scheme rs-1x
```

4） 检查AC上的服务器IP地址是否配置正确，nas-ip地址与Key与服务器端配置是否一致。

6 检查服务器上相关配置

检查接入设备的ip地址是否写错，共享秘钥是否与AC上配置的一致、核查接入用户的信息，账户名和密码是否有误，是否配置相同账号允许至少两个用户同时在线等

7 优化1x细节配置

如有1x认证偶发失败、网络环境较差的场景，可以参考如下1x优化配置：

dot1x timer tx-period 4 （缺省30s）

该命令用来调整设备重传EAP-Request报文的时间间隔，也就是当设备向无线客户端发送了EAP-Request报文后，如果在这个时间内没有收到EAP-Response报文，会重新发送EAP-Request报文，如果总发送次数达到retry指定的次数则认证失败； 该配置默认为30s，配置后缩短设备报文重传间隔，降低终端由于响应不及时而认证失败的概率。

dot1x timer supp-timeout 2 （缺省30s）

dot1x retry 10 （缺省2次）

在实际应用中，802.1x客户端的实现存在很大的差别，也就是说当AP发送了EAP-Request报文后，在一定的时间内可能无线客户端无法及时响应EAP-Response报文，最终导致认证无法成功；为了减少这种情况，在具体实施中我们可以适当调整supplicant的时间和retry的次数，来减少这种终端无法及时响应进而认证失败的情况；

wlan client-security authentication clear-previous-connection

（已认证无线客户端再次上线认证清除旧连接功能）

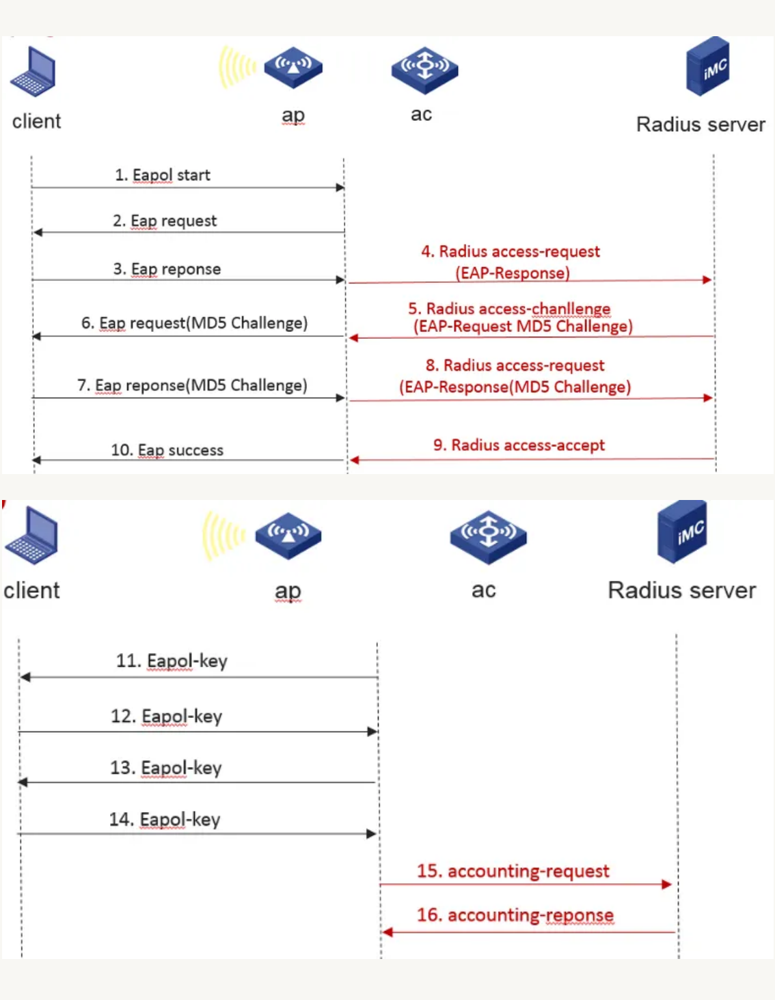
漫游场景下，假设终端从AP1漫游到AP2，在这个漫游过程中，可能出现终端先与AP2关联并进行802.1X认证上线，再与AP1去关联，从而引起与Radius服务器交互时出现，计费先开始后停止的报文交互，此时可能引起Radius服务器逻辑混乱，判定终端重复认证进而导致认证失败而下线。开启该功能后，在客户端上线发认证请求报文之前先发计费停止报文，解决由于终端漫游而让服务器认为是重复认证导致终端下线的情况。

8 如还不能定位故障怎么办？

可以通过收集802.1x认证过程中的debug信息，我们通过报文的交互流程来进一步的查看问题：

```
debugging radius all
debugging dot1x all
debugging wlan client mac XXXX
debugging wlan access-security all
debugging wlan usersec all
```

1x认证流程（中继模式）：



Tips

有线1x和无线1x认证有什么区别?

对于802.1x认证本身，无线用户和有线用户没有任何的差别，只是无线用户在认证成功后会使用认证过程中产生的radius key生成后续4-way handshake的种子密钥。

4-way handshake可以作为802.1x协议的一部分，是专门为WLAN设计，通过802.1x的EAPOL-Key报文完成无线客户端和设备之间的密钥协商。

当上面的所有过程完成后，该无线客户端才会认为成功接入到WLAN服务中；如果任何一个环节出现错误都会被认为无线认证结果失败，AP会主动发送Disassociation报文将该无线客户端断开；

因此由于无线的1x认证涉及秘钥协商的过程，所以如果想实现无线终端1x认证失败放入fail vlan内、认证失败后实现**逃生等需求**是无法满足的，只能通过新建逃生ssid解决。

<宠粉走起来>

更多感兴趣的无线专题 **猛戳评论区留言给小编~**

想了解更多无线知识可以复制下方链接或点击阅读全文，欢迎下载学习《无线V7一本通V2.0》，《小贝无线一本通V1.0》，无线维护的好帮手！

http://h3c.com/cn/Service/Document_Software/TechnicalInfo/PorductMaintanInfo/WLAN/DailyMainten/DailyMaintenGuide/

往期公众号PDF合集：知了社区— 运维工具—资料中心—无线—《冬冬说无线》系列资料

冬冬说无线　　下期再见~！

PS：官方技术支持热线，请拨打400-810-0504

更多内容，请关注

▽

球分享　球点赞　球在看